REMARKS

Claims 1-3, 6, 10, 11, 16, 21, 22, 24, and 26 are proposed for amendment herein. Claims 1-3, 6-12, 14-24 and 26-27 are presently pending in the above-identified application.

Telephone Discussion – June 3, 2005

Applicants wish to the thank Examiner Zia for the time and courtesies extended to Applicants' undersigned attorney in the telephone conversation of June 3, 2005 to discuss the disposition of the current application. To that end, Applicants present this Amendment that contains a response to the outstanding rejections and amends the claims to even further distinguish over the cited prior art. The amended claims also include language to address some of the points expressed by the Examiner in the June 3 telephone conversation.

Applicants respectfully submit, in view of this Amendment, that each of the currently pending claims, as amended, is patentably distinct from the cited prior art and in condition of allowance. As discussed on the telephone call, Applicants understand that prior to issuing the next Office communication in the present application Examiner will conduct a telephonic interview with the undersigned Attorney should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance.

Claim Objections

The Office Action objected to claim 6. Applicants have amended claim 6 herein to correct the dependency of such claim and respectfully request the withdrawal of this objection.

Rejection of Claims under 35 USC § 112

The Office Action rejected claims 1, 10, 16, 21 and 24 under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement, in particular, with respect to the claimed "security characteristic" and "an indication of connectivity"

subject matter, and asserts that "the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.." (see, Office Action, page 5). Similarly, the Office Action rejected claims 7, 20 and 23 as failing to comply with the enablement requirement with respect to the claimed "different security levels". Applicants respectfully disagree as discussed below.

With respect to the claimed "security characteristic" subject matter, Applicants direct the Examiner's attention to at least the following passages in Applicants' Specification: (i) page 10, line 5-28; (ii) page 6, lines 10-26; (iii) page 5, lines 1-6; (iv) page 2, line 28 through page 3, line 10 and (v) page 1, line 28 through page 2, line 10. At a minimum, such passages from Applicants' Specification (in combination with the entire disclosure therein) enable one skilled in the art to recognize that the "security characteristic" subject matter of Applicants' claimed invention is directed to identifying potential security risks across the perimeter of a network (see, e.g., Applicants' Specification, page 4, lines 27-30; and page 8, lines 17-22) which, in turn, is the "determining a security characteristic of the probed host" as claimed by Applicants. That is, the security characteristic of the probed host, in accordance with the invention, is whether such probed host poses a security risk across the perimeter of the its associated network as supported by the above-referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use the claimed security aspects of Applicants claimed invention.

With respect to the claimed "an indication of connectivity" subject matter, Applicants direct the Examiner's attention to at least the following passages in Applicants' Specification: (i) page 5, lines 1-6; (ii) page 5, lines 26-29; (iii) page 8, lines 17-22; and (iv) page 9, line 15 through page 11, line 14. At a minimum, such passages from Applicants' Specification (in combination with the entire disclosure therein) enable one skilled in the art to recognize that the "an indication of connectivity" subject matter of Applicants' claimed invention is directed discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically configured probe packet. As will be recognized by one skilled in the art the

"connectivity" aspect of the invention is the existence of, or absence of, a connection, as supported by the above-referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use the security aspects of Applicants' claimed invention.

With respect to the claimed "different security levels" subject matter, Applicants direct the Examiner's attention to at least the following passages in Applicants' Specification: (i) page 6, lines 1-9; (ii) page 6, lines 10-26; and (iii) page 8, lines 5-7. At a minimum, such passages from Applicants' Specification (in combination with the entire disclosure therein) enable one skilled in the art to recognize that the "different security levels" subject matter of Applicants' claimed invention is directed to the aspect of the invention that ascertains the security of different types of networks, e.g., an intranet vs. the Internet, or a corporate backbone vs. an external network. One skilled in the art will clearly recognize that such disparate networks may have "different security characteristics" which are well-known and specified by the network's system administrators for example, as supported by the above-referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use Applicants' claimed invention.

In view of the above, Applicants respectfully submit that the claimed "security characteristic", "an indication of connectivity" and "different security levels" subject matter is supported by Applicants' Specification and compliant with the enablement requirements of 35 USC § 112, first paragraph, and respectfully request the withdrawal of these claim rejections.

Rejection of Claims under 35 USC § 102(e)

The Office Action rejected claims 1-3, 6-12 14-24 and 26-27 under 35 USC § 102(e) as being anticipated by U.S. Patent No. 6,298,445 issued to A. Shostack et al. (hereinafter "Shostack"). Applicants have amended the claims herein to more particularly claim the various aspects of the invention, and respectfully submit that each of the currently pending is patentably distinct from Shostack.

As discussed in prior Amendments in the present application, Applicants' claimed invention is directed at ascertaining the integrity of a communications network and thereby identifying potential security risks across the perimeter of such network. Thus, an aspect of the invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured with a source address which is associated with the second communications network, and the connectivity measure is determined as function of a response from the probed host (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, lines 20-22) to the packet.

Importantly, the source address is selected such that the IP address is external to the probed host's network, that is, the originator address is "false or derived" in that it does not originate from an actual host request (see, e.g., Applicants' Specification, page 9, lines 25-29). Thus, in accordance with claimed invention, as more particularly set forth in the amended claims herein, the source address is selected independent of any request from the second host to the first host. Thus, by probing the connectivity of the particular host(s) within a network, in accordance with the claimed invention, an analysis of the network can be made to identify potential security risks across the perimeter of the particular network.

Said another way, Applicants' claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically configured probe packet. In brief, it is the

determination of such connectivity measure, using the probe packet configured in accordance with the invention that is the contribution advanced by the Applicants over the cited prior art. Applicants have realized that spoofed packets can serve different purposes (and non-malicious) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by system administrators to identify potential security risks across a network's perimeter and prevent malicious attacks (including but not limited to malicious spoofing).

Applicants have amended the pending independent claims to more particularly claim the above-described aspects of the invention. For example, amended independent claim 1 recites:

> "A communications network security method for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the method comprising:
>
> identifying a plurality of routes that define the first communications network;
>
> identifying a plurality of hosts associated with the first communications network as a function of the plurality of routes;
>
> receiving a census of the first communications network as a function of the plurality of hosts to determine a topology of the first communications network;
>
> probing at least one first host of the plurality hosts of the first communications network by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and
>
> determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications

network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network." (emphasis added by Applicants)

Each of the currently pending independent claims has been amended in a similar fashion as the above-referenced amended independent claim 1 to contain similar limitations directed to the above-described features of the invention.

It is at least the above-described aspects of Applicants' invention that stand in contrast to the cited Shostack reference. Specifically, in addition to the discussion of Shostack in the prior Amendments, Applicants' respectfully submit that Shostack teaches a technique for testing for susceptibility to various so-called security vulnerabilities, such security vulnerability including IP spoofing. For example, Shostack at column 12, lines 50-55 describes an aspect of Shostack's technique which "...probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited...". Shostack's "security vulnerabilities", as referenced throughout such disclosure, are of the type listed in Shostack's Table 1 (see, e.g., Shostack, columns 5 and 6). While it is true that one such Shostack security vulnerability is a "check of the firewall for IP spoofing" (see, Shostack, column 5, lines 59-60) or "...assess the security vulnerabilities of a remote computer connected to the network..." (see, Shostack, column 13, lines 2-3), these are not disclosures that are fatal to the novelty of Applicants' claimed invention.

In support of the outstanding rejection of Applicants' pending claims, the Office Action on page 3 includes:

> "...Cited prior art teaches a fourth module of this system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service. Examiner references column 12, lines 41-57 as the teaching of what module two does. Specifically module two carries the network scan and generates a map of the network and scans the ports for known security vulnerabilities. Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network. (Emphasis added by Applicants); and
>
> "Cited prior art also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a similar system over a computer network. In line 27, the module invokes

> remote systems. In line 34, Shostack teaches that this sixth [module] checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions of Shostack's invention.." (emphasis added by Applicants); and
>
> "The Examiner has pointed to two separate teachings where Shostack teaches or suggests utilizing a probe packet to determine a connectivity measure between the two communication network where the packet includes a source address which is associated with a second communications network..."

Applicants submit that Shostack's fourth module (and, for that matter Shostack's second or sixth module) is not performing (and does not anticipate, teach or suggest) Applicants' claimed invention. In particular, the fact that Shostack's fourth module essentially implements—on a remote basis—the functionality of the second module does not teach or suggest Applicants' claimed invention. Shostack, at column 12, lines 41-55, teaches:

> "...The second module 76 accesses the database of security vulnerabilities 92 and assesses network security. The second module 76 connects to a network service, accepts information from the service and interrogates the service. The second module 76 performs a network scan and...The network scan produces a map of the network 86 which is essentially an inventory of the Internet Protocol (IP) devices connected to the network. Using network protocol, the integrate system also probes the ports of each of the IP devices for programs that contain security vulnerabilities that may be exploited.. The network scan ensures that the network 20 and a local server 18 is protected against any unauthorized access that may penetrate the firewall 12...." (emphasis added by Applicants)

Again, the Office Action is relying on the above features of Shostack's second module and the "remote" action of Shostack's fourth module to support the rejection of Applicants claimed invention. Applicants do not dispute that Shostack's fourth module allows a remote computer to first connect to a network service then accepts information from the service and like the second module also interrogates the services (see, e.g., Shostack, column 13, line 3-6). Applicants do dispute that such teaching anticipates the claimed invention herein.

In particular, as pointed out in the Office Action Shostack's fourth (and second) module require a connection from the remote (or local) computer and after the establishment of such connection, such modules "interrogate" the network service in

accordance with Shostack's security vulnerabilities. In contrast, Applicants' claimed invention does not require the establishment of any such connection. That is, Applicants' claimed invention is directed to determining whether a connection exists between a host on a first network and as host on a second network utilizing the probe packet configured in accordance the claimed invention. As such, Applicants' invention might by useful in Shostack's system to determine whether the connection, for example, between Shostack's fourth module (or another host computer in the fourth module's network) and the remote computer (on a second network, for example) is proper and not a rogue connection, which may present a potential security risk across the network's perimeter.

Further, Shostack's sixth module teaches a "communications module" which performs well-known system functions such as maintaining communication between Shostack's modules and/or other similar systems, database sharing, report generation/analysis, security and checking the integrity of existing service connections (see, e.g., Shostack, column 13, lines 18-36).

Neither of these modules (i.e., Shostack second, fourth or sixth modules) employs the configured probe packet, as claimed by Applicants, to determine a connectivity measure between two communication networks (where the packet includes a source address which is associated with a second communications network), wherein the source address is selected independent of any request from the second host to the probed host, which can be used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and the host on a second communications network.

Regarding the rejection of each of the presently pending dependent claims these claims depend ultimately from one of the pending amended independent claims 1, 10, 16, 21 and 24 herein which Applicants submit are patentably distinct over Shostack for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Shostack for the aforesaid reasons, as well as other elements these claims add in combination to their base claim.

Therefore, in view of the foregoing, Applicants respectfully submit that each of the currently pending claims, as amended, is patentably distinct from Shostack. As such, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Steven Branigan
Hal Joseph Burch
William R. Cheswick

By _____
Donald P. Dinella
Attorney for Applicants
Reg. No. 39,961
908-582-8582

Date: June 7, 2005

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030